In the Specification

Please replace the paragraph that begins on Page 1, line 4 and carries over to Page 2, line 4 with the following marked-up replacement paragraph:

-- The present invention is related to the following commonly-assigned U. S. ~~Patents~~ Patent Applications, all of which were filed on 12/05/2001 and which are hereby incorporated herein by reference: U. S. Patent Application serial ~~Patent _____ (serial~~ number 10/007,593[[)]], entitled "Kernel-Based Security Implementation"; U. S. Patent Application serial ~~Patent _____ (serial~~ number 10/007,446[[)]], entitled "Policy-Driven Kernel-Based Security Implementation"; U. S. Patent Application serial ~~Patent _____ (serial~~ number 10/007,582[[)]], entitled "Offload Processing for Secure Data Transfer"; and U. S. Patent Application serial ~~Patent _____ (serial~~ number 10/007,581[[)]], entitled "Offload Processing for Security Session Establishment and Control". These U. S. ~~Patents~~ Patent Applications are referred to hereinafter as "the related inventions". The present invention is also related to commonly-assigned U. S. Patent Application serial ~~Patent _____ (serial~~ number 10/058,870 (now U. S. Patent 7,076,803), entitled "Integrated Intrusion Detection Services", which was filed concurrently herewith. --

Please replace the paragraph on Page 33, lines 16 - 19 with the following marked-up replacement paragraph:

-- Using these types of locally-available details in determining whether an attack is indicated enables more accurate determinations, thereby decreasing false ~~positives~~ positive notifications. Increasing intrusion detection sensitivity without increasing false positives is a

noteworthy goal of intrusion detection techniques. --

Please replace the paragraph on Page 39, lines 1 - 6 with the following marked-up replacement paragraph:

-- Having completed IP processing, the packet continues upward through the protocol stack (minus its IP headers), and reaches the TCP/UDP/ICMP or other protocol processing layer (Block 1025). Block 1030 checks to see if the data for TCP/UDP layer is encrypted. If so, decryption is performed (Block 1035). Block 1040 compares the unencrypted TCP/UDP packet to the known attack signatures for the TCP/UDP layer. The TCP/UDP processing is then completed, as shown by Block [[1020]] 1045. --

Please replace the paragraph on Page 40, lines 13 - 17 with the following marked-up replacement paragraph:

-- In Block 1200, the inline packet processing logic is entered as the packet traverses through the stack. Block 1205 tests whether an error has been detected for this packet. (As was described above for Block 1105, this test may pertain to normal error handling and/or signature comparisons.) If there is no detected error, then control transfers to Block 1235, which indicates that the packet processing is completed. Fig. 12 then exits (Block 1240). --